WHAT IS CLAIMED IS:

1. A method of implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$ and in which x and y are variables in an x-y coordinate system, a and b are parameters, addition of points P1(x1, y1) and P2(x2, y2) on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by P3(x3, y3) with subtraction of said points P1(x1, y1) and P2(x2, y2) being presumed to be represented by P4(x4, y4), comprising the steps of:

inputting the coordinate component x1;

transforming said inputted coordinate component x1 into X- and Z-coordinates $[X_1, Z_1]$ of a projective space where Z is a variable in the Z-coordinate;

storing said coordinates $[X_1, Z_1]$ of said projective space;

transforming said coordinate component x2 into coordinates $[X_2, Z_2]$ of said projective space;

storing said projective coordinate $[X_2, Z_2]$;

transforming said coordinate component x4 into coordinates $[X_4, Z_4]$ of said projective space;

storing said projective coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates $[X_3,$

Z_3] into said coordinate component x3; and

outputting said coordinate component x3,

whereby scalar multiplication of said point P1(x1, y1) is determined.

2. A method of implementing an elliptic curve cryptography according to claim 1,

further comprising the steps of:

generating a random number $\underline{k}$;

storing said generated random number $\underline{k}$;

transforming the x-coordinates into projective coordinates to thereby derive projective coordinates [k^2x, k] through arithmetic operation of individual coordinate components of said projective space and said stored random number $\underline{k}$.

3. A method of implementing an elliptic curve cryptography according to claim 1,

further comprising the steps of:

generating a random number $\underline{k}$;

storing said generated random number $\underline{k}$;

transforming the x-coordinates into projective coordinates to thereby derive projective coordinates [kx, k] through arithmetic operation of individual coordinate components of said projective space and said stored random number $\underline{k}$.

4. A method of implementing an elliptic curve cryptography according to claim 1,

wherein the step of determining said projective coordinates [X_3, Z_3] susceptible to the transformation

into said coordinate component x3 from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ includes the substeps of:

computing $B = X_1Z_2^2 + X_2Z_1^2$;

storing said computed B;

deciding whether or not said stored B satisfies condition that $B = 0$;

outputting a point at infinity when $B = 0$ while arithmetically determining $Z_3 = Z_4B$ unless $B = 0$;

storing said determined Z_3; and

arithmetically determining $X_3 = X_4B^2 + X_1X_2Z_1^2Z_2^2Z_4^2$ from said stored Z_3.

5. A method of implementing an elliptic curve cryptography according to claim 1,

wherein the step of determining said projective coordinates $[X_3, Z_3]$ susceptible to transformation into said coordinate component x3 from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$ includes the substeps of:

computing $B = X_1Z_2 + X_2Z_1$;

storing said computed B;

deciding whether or not said stored B satisfies condition that $B = 0$; and

outputting a point at infinity when $B = 0$ while determining arithmetically $Z_3 = Z_4B^2$ and $X_3 = X_4B^2 + X_1X_2Z_1Z_2Z_4$ unless $B = 0$.

6. An apparatus implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an

extension field of "2"), in which x and y are variables in an x-y coordinate system, a and b are parameters, said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$, comprising:

random number generating means for generating a random number k;

projective coordinate transformation means receiving as inputs thereto coordinate x0 of said finite field of characteristic 2 and said random number k, to thereby transform said coordinate x0 into projective coordinates $[kx0, k] = [X_1, Z_1]$;

doubling arithmetic means for arithmetically determining a double point from said projective coordinates $[X_1, Z_1]$;

addition arithmetic means for determining an addition point from said projective coordinate $[X_1, Z_1]$ where Z is a variable in the Z-coordinate to thereby output said addition point; and

scalar multiplication means receiving information from said projective coordinate transformation means, said doubling arithmetic means and said addition arithmetic means to thereby perform scalar multiplication of the coordinate component x0.

7. A recording medium storing a program for implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$ and in which x and y are variables in an x-y

coordinate system, a and b are parameters, addition of points P1(x1, y1) and P2(x2, y2) on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by P3(x3, y3) with subtraction of said points P1(x1, y1) and P2(x2, y2) being presumed to be represented by P4(x4, y4), said program comprising the statements of:

inputting an coordinate component x1;

transforming said inputted coordinate component x1 into X- and Z-coordinates $[X_1, Z_1]$ in a projective space;

storing said coordinates $[X_1, Z_1]$ of said projective space;

transforming said coordinate component x2 into coordinates $[X_2, Z_2]$ of said projective space;

storing said projective coordinate $[X_2, Z_2]$ where Z is a variable in the Z-coordinate;

transforming said coordinate component x4 into coordinates $[X_4, Z_4]$ of said projective space;

storing said projective coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates $[X_3, Z_3]$ into said coordinate component x3; and

outputting said coordinate component x3,

whereby scalar multiplication of said point P1(x1, y1) is determined.

8. A recording medium storing a program for implementing an elliptic curve cryptography according to claim 7,

said program further comprising the statements of:

generating a random number $\underline{k}$;

storing said generated random number $\underline{k}$;

transforming the x-coordinates into projective coordinates to thereby derive projective coordinates $[k^2x, k]$ through arithmetic operation of individual coordinate components of said projective space and said stored random number $\underline{k}$.

9. A recording medium storing a program for implementing an elliptic curve cryptography according to claim 7,

said program further comprising the statements of:

generating a random number $\underline{k}$;

storing said generated random number $\underline{k}$;

transforming the x-coordinates into projective coordinates to thereby derive projective coordinates $[kx, k]$ through arithmetic operation of individual coordinate components of said projective space and said stored random number $\underline{k}$.

10. A recording medium storing a program for implementing an elliptic curve cryptography according to claim 7,

wherein the said statement of determining said

projective coordinates [X_3, Z_3] susceptible to transformation into said coordinate component x3 from said stored projective coordinates [X_1, Z_1], [X_2, Z_2] and [X_4, Z_4] includes further the statements of:

computing $B = X_1Z_2^2 + X_2Z_1^2$;

storing said computed B;

deciding whether or not said stored B satisfies condition that B = 0;

outputting a point at infinity when B = 0 while determining arithmetically $Z_3 = Z_4B$ unless B = 0;

storing said determined Z_3; and

determining arithmetically X_3 $= X_4Z_3^2 + X_1X_2Z_1^2Z_2^2Z_4^2$ from said stored Z_3.

11. A recording medium storing a program for implementing an elliptic curve cryptography according to claim 7,

wherein the statement of determining said projective coordinates [X_3, Z_3] susceptible to transformation into said coordinate component x3 from said stored projective coordinates [X_1, Z_1], [X_2, Z_2] and [X_4, Z_4] includes further the statements of:

computing $B = X_1Z_2 + X_2Z_1$;

storing said computed B;

deciding whether or not said stored B satisfies condition that B = 0; and

outputting a point at infinity when B = 0 while determining arithmetically $Z_3 = Z_4B^2$ and X_3 $= X_4B^2 + X_1X_2Z_1Z_2Z_4$ unless B = 0.

12. A computer program, on a medium for implementing an elliptic curve cryptography in a finite field of characteristic 2 (or an extension field of "2"), in which said elliptic curve is given by $y^2 + xy = x^3 + ax^2 + b$ and in which x and y are variables in an x-y coordinate system, a and b are parameters, addition of points P1(x1, y1) and P2(x2, y2) on said elliptic curve composed of points defined by individual coordinate components is presumed to be represented by P3(x3, y3) with subtraction of said points P1(x1, y1) and P2(x2, y2) being presumed to be represented by P4(x4, y4), said program comprising the statements of:

inputting an coordinate component x1;

transforming said inputted coordinate component x1 into X- and Z-coordinates $[X_1, Z_1]$ in a projective space;

storing said coordinates $[X_1, Z_1]$ of said projective space;

transforming said coordinate component x2 into coordinates $[X_2, Z_2]$ of said projective space;

storing said projective coordinate $[X_2, Z_2]$ where Z is a variable in the Z-coordinate;

transforming said coordinate component x4 into coordinates $[X_4, Z_4]$ of said projective space;

storing said projective coordinates $[X_4, Z_4]$;

determining projective coordinates $[X_3, Z_3]$ from said stored projective coordinates $[X_1, Z_1]$, $[X_2, Z_2]$ and $[X_4, Z_4]$;

transforming said projective coordinates [X_3, Z_3] into said coordinate component x3; and

outputting said coordinate component x3,

whereby scalar multiplication of said point P1(x1, y1) is determined.